第7回

連載　プライバシー・サイバーセキュリティと企業法務

取引先のサイバーセキュリティを確保する上での留意点

弁護士
山岡裕明 Hiroaki Yamaoka

連載企画／
弁護士　**渡邊涼介**・弁護士　**山岡裕明**

I　総論

企業法務においてプライバシー及びサイバーセキュリティを検討する際、自社における体制整備が出発点となる。プライバシーについていえば、第6回で紹介したとおりプライバシー情報が漏えいした場合に自社が不法行為上の責任を負いかねないことを念頭に、自社内においてプライバシー情報を適切に取り扱う体制を整備することとなる。サイバーセキュリティについても同様で、自社がサイバー攻撃を受けた場合に負担を余儀なくされる損害や法的責任を念頭に置きつつ、サイバーリスクが顕在化しないようにサイバーセキュリティ体制の整備を進める。

もっとも、DX化が進み企業がITインフラへの依存を高め、かつ、各種電子データの共有が容易となっている状況下においては、自社の体制を整備するだけでは十分とはいえなくなりつつある。例えば、第3回で記載したとおり、近時のランサムウェア攻撃においては、企業内のネットワークに侵入してファイルサーバから大量の電子ファイルを外部に送信して窃取する。このファイルサーバには個人データだけではなく、設計図、ソースコード、開発データ、契約書、財務書類など事業活動に関わる重要な電子ファイルも多数含まれる。いくら自社のセキュリティ体制を整備していたとしても、取引先がランサムウェア攻撃を受けると自社の電子ファイルが窃取されかねない。また、同じく取引先がランサムウェア攻撃を受けて一時的に事業停止に追い込まれた場合、製品の納品やサービスの提供を受けることができなくなる。その結果、自社の製造やサービスも一時的に停止せざるを得なくなることが想定される。しかも、製造業の分野では、高度に複雑化したサプライチェーンが発達しているため、直接の取引先に限られず、サプライチェーンのうちの一社がランサムウェア攻撃を受けて工場が停止した場合、その影響は当該一社にとどまらず、サプライチェーン全体に対し、事業の一時停止などの悪影響が波及するおそれがある。

実際に、トヨタ自動車株式会社（以下「トヨタ社」という。）は、部品仕入取引先の小島プレス工業株式会社（以下「小島プレス社」という。）のシステム障害を受けて、2022年3月1日、国内全工場の稼働を停止することとなった[1]。詳細は不明であるが、これは、サプライヤーである小島プレス社がサイバー攻撃を受けてシステ

1　トヨタ社プレスリリース（https://global.toyota/jp/newsroom/corporate/36960974.html）。